

Security

Industrial Security Program

Headquarters
Department of the Army
Washington, DC
15 April 1982

UNCLASSIFIED

SUMMARY of CHANGE

AR 380-49

Industrial Security Program

Effective 15 May 1982

Security

Industrial Security Program

By Order of the Secretary of the Army:

E. C. MEYER
General, United States Army
Chief of Staff

Official:

ROBERT M. JOYCE
Brigadier General, United States Army
The Adjutant General

History. This publication has been reorganized to make it compatible with the Army electronic publishing database. No content has been changed.

Summary. This revision implements DOD

Directive 5220.22, DOD Industrial Security Program, and DOD 5220.22–R, DOD Industrial Security Regulation (ISR).

Applicability. Not Applicable.

Proponent and exception authority. Not Applicable.

Army management control process. Not Applicable.

Supplementation. Local limited supplementation of this regulation is permitted but is not required. If supplements are issued, HQDA agencies and major Army commands will furnish one copy of each to HQDA(DAMI–CIS), WASH DC 20310; other commands will furnish one copy of each to the next higher headquarters.

Interim changes. Interim changes to the regulation are not official unless they are authenticated by The Adjutant General. Users

will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the Office of the Assistant Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) direct to HQDA (DAMI–CIS), WASH DC 20310.

Distribution.

To be distributed in accordance with DA Form 12–9A requirements for AR, Security:

Active Army: D

ARNG: None

USAR: D

Contents (Listed by paragraph and page number)

Purpose. • 1, *page 1*

Applicability. • 2, *page 1*

Explanation of terms. • 3, *page 1*

References. • 4, *page 1*

Responsibilities. • 5, *page 1*

Concept of operations. • 6, *page 1*

Administration. • 7, *page 1*

Release of classified intelligence information to contractors. • 8, *page 1*

Classification guidance. • 9, *page 1*

Security of classified contracts performed on Army installations. • 10, *page 1*

Appendixes

A. References, *page 4*

B. Supplemental Instruction for the Use of DOD 5220.22–R, Industrial Security Regulation (ISR), *page 4*

C. Information Regarding Cognizant Security Offices, DISCO, DISI, and OISI, *page 9*

Glossary

*This regulation supersedes AR 380–49, 10 March 1977.

RESERVED

1. Purpose.

This regulation provides instructions and policy guidance on the following:

- a. DA Industrial Security Program (referred to hereafter as the program).
- b. Security of classified information possessed by US industry.
- c. Standardization of industrial security measures throughout the Army.
- d. Maintenance of maximum security for the program, consistent with the assigned missions of Army elements.

2. Applicability.

This regulation applies to the Active Army. It does not apply to the Army National Guard and the US Army Reserve.

3. Explanation of terms.

Special terms used in this regulation are explained in the glossary. The glossary also explains terms commonly used in industrial security.

4. References.

Required publications are listed in appendix A.

5. Responsibilities.

a. The Deputy Under Secretary of Defense (Policy) (DUSD(P)) provides overall policy guidance for the program, in accordance with DOD 5220.22-R(ISR).

b. The Director of the Defense Investigative Service (DIS) does the following:

- (1) Administers the program, under the provisions of the ISR.
- (2) Assumes security cognizance for all contractors and industrial facilities under the program, according to the provisions of the ISR.
- (3) Keeps the Assistant Chief of Staff for Intelligence (ACSI) informed of significant aspects of the program.

c. ACSI. The ACSI is the implementing agent for the program throughout the Army. The ACSI will—

- (1) Coordinate policies outlined in this regulation with the Office of the DUSD(P), the DIS Director, and other Military Departments and agencies involved in the program.
- (2) Ensure that standardization of the program is maintained throughout the Army when informed by the DIS Director of significant developments in the program.

6. Concept of operations.

a. The provisions of the ISR apply to DA activities in their industrial security relationships with industry. The ISR sets forth internal DOD policies and procedures for safeguarding classified information entrusted to contractors. These include foreign and international pact organizations' classified information which the US Government is obliged to protect for national security reasons. (Supplemental instructions for the use of the ISR are found at app B.)

b. DOD 5220.22-M (DOD Industrial Security Manual for Safeguarding Classified Information (ISM)) contains detailed instructions for contractors in safeguarding classified information. The ISM is a companion publication to the ISR. It is made applicable to the program in the following provisions:

- (1) By execution of a DOD Security Agreement (DD Form 441). This form is explained in the ISR.
- (2) By reference in the "Military Security Requirement" clause in the contract.

7. Administration.

The program for contracts awarded by DA, and for the resulting industrial security program, is administered jointly by the DIS Director and the ACSI, in accordance with the ISR. The ISR and the ISM provide guidelines on administration; these guidelines are summarized as follows:

a. Within DIS, the director for industrial security administers the following:

(1) *Security cognizance.* DIS regional directors have the authority to administer the program within their regions. Regional directors of industrial security have been designated as cognizant security officers for all US Contractor Facilities in their geographical regions on behalf of DA. (See paras 1-108, 1-115, and 1-305 of the ISR, and app C.)

(2) *Security clearance.* The DIS Director administers the program's investigative and individual security clearance functions.

(a) *Facility clearances.* Each DIS regional cognizant security officer will process and grant clearances on contractor facilities. Inquiries concerning the clearance status and storage capability of a particular facility will be directed to the DIS regional officer having jurisdiction over the facility.

(b) *Personnel clearances.* Except for CONFIDENTIAL clearances granted by the contractor, all industrial security personnel clearances required under the program are granted for the government by the Defense Industrial Security Clearance Office (DISCO). CONFIDENTIAL clearances granted by the contractor are valid only while employed at a facility of the contractor organization. They are not valid for access to Restricted Data; communications security (COMSEC) information; sensitive compartmented information; and arms control disarmament agency classified information, except for NATO restricted information. Inquiries on security clearances of contractor employees will be directed to: Chief, DISCO (ATTN: Central Index File), P.O. Box 2499, Columbus, OH 43216.

b. In DA contracting agencies, contracting officers will appoint persons to serve as points of contact (POC). These POCs will coordinate and act on industrial security matters; they also will execute industrial security functional responsibilities of the contracting officer. (See app C, ISR).

8. Release of classified intelligence information to contractors.

Procedures governing the control of dissemination of classified intelligence information and the release of classified intelligence information to contractors are prescribed in AR 381-1.

9. Classification guidance.

Army contracting agencies will provide classification guidance to contractors, as required by the ISR. The "Contractor Security Classification Specification" (DD Form 254) will convey specific guidelines for each classified contract. (Fig. 1 shows a sample DD Form 254 format). Information concerning the preparation of classification guidance is contained in DOD 5220.22-H and DOD 5200.1-1. (See also app E, AR 380-5.)

10. Security of classified contracts performed on Army installations.

a. The installation commander will provide for the security of classified contracts performed on the installation. Exceptions are when—

- (1) The contractor activity has been designated a contractor facility.
- (2) The installation commander has elected not to perform the security functions listed in paragraph 1-108b of the ISR.

b. The installation commander continues to retain overall responsibility for the security of the installation. Specific installation security requirements will be included in contracts, as applicable.

(S A M P L E)

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS <u>SECRET</u>	
2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	4. DATE TO BE COMPLETED (Estimated)
X a. PRIME CONTRACT		b. PRIME CONTRACT NUMBER DAAH 01-79-C 0001	a. 1 Nov 80
b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier)		b. FIRST TIER SUBCONTRACT NO.	b. <input type="checkbox"/> ORIGINAL (Complete date in all cases) <input checked="" type="checkbox"/> REVISED (Supersedes all previous specifications)
c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION		c. IDENTIFICATION NUMBER	c. DUE DATE
6. Is this a follow on contract? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If YES, complete the following:		a. DAAH 01-78-C 0004 b. 30 Oct 79 c. Accountability for classified material on preceding contract	
7a. Name, Address & Zip Code of Prime Contractor *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
XYZ Production Corporation 10 Main Street Los Angeles, CA 90015		54321	Defense Contract AOM Serv Reg 11099 Slacienegge Blvd Los Angeles, CA 90045
8a. Name, Address & Zip Code of First Tier Subcontractor *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
* When actual performance is at a location other than that specified, identify such other location in item 15.			
10a. General identification of the Procurement for which this specification applies		b. DoDAAD Number of Procuring Activity identified in item 16d	
Production of STINGER/STINGER-POST Guided Missile System		X123	
c. Are there additional security requirements established in accordance with paragraph 1.114 or 1.115, ISR? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If YES identify the pertinent contractual documents in item 15.			
d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If YES explain in item 15 and identify specific areas or elements.			
11. ACCESS REQUIREMENTS		YES	NO
a. Access to Classified Information Only at other contractor/Government activities			X
b. Receipt of classified documents or other material for reference only (no generation)			X
c. Receipt and generation of classified documents or other material.		X	
d. Fabrication/Modification/Storage of classified hardware		X	
e. Graphic arts services only.			X
f. Access to IPO information.			X
g. Access to RESTRICTED DATA.		X	
h. Access to classified COMSEC information.			X
i. Cryptographic Access Authorization required.			X
ACCESS REQUIREMENTS (Continued)		YES	NO
j. Access to SENSITIVE COMPARTMENTED INFORMATION			X
k. Access to other Special Access Program information (Specify in item 15).			X
l. Access to U. S. classified information outside the U. S., Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.			X
m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.			X
n. Classified APP processing will be involved.			X
o. REMARKS:			
12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (item 15e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).			
a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.			
b. Typed name, title and signature of program/project manager or other designated official		c. Activity name, address, Zip Code, telephone number and office symbol	
JOHN J. DOE Contracting Officer for Security		STINGER Missile Project Office (SMPO) US Army Missile Command Redstone Arsenal, AL 35809 (504) 123-4567	
NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.			

DD FORM 254
1 JAN 78

EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

Figure 1. Example of a completed DA Form 254.

(S A M P L E)

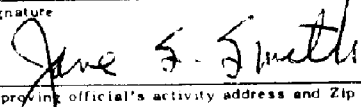
13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual (paragraph 5c and Appendix IX).	
b. Proposed public releases shall be submitted for approval prior to release. <input type="checkbox"/> Direct <input checked="" type="checkbox"/> Through (Specify): <div style="text-align: center; padding: 5px;">Addressee in 12b</div> <p style="font-size: small;">to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs), * for review in accordance with paragraph 5c of the Industrial Security Manual. * In the case of non-DoD User Agencies, see footnote, paragraph 5c, Industrial Security Manual.</p>	
14. Security Classification Specifications for this solicitation contract are identified below ("X" applicable boxes) and supply attachments as required. Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide: (I) Category of classification; (II) Date or event for declassification or review for declassification; and (III) The date or event for downgrading (if applicable). The official named in Item 12b is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.	
<input type="checkbox"/> a. A completed narrative is (1) <input type="checkbox"/> attached, or (2) <input type="checkbox"/> transmitted under separate cover and made a part of this specification. <input checked="" type="checkbox"/> b. The following classification guide(s) is made a part of this specification and is (1) <input type="checkbox"/> attached, or (2) <input checked="" type="checkbox"/> transmitted under separate cover. (List guides under Item 15 or in an attachment by title, reference number and date). <input type="checkbox"/> c. Service type contract/subcontract. (Specify instructions in accordance with ISR/ISM, as appropriate). <input type="checkbox"/> d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____. <input checked="" type="checkbox"/> e. XXXX Biennial review of this DD Form 254 is required. If "X'd" provide date such review is due: <u>1 May 1980</u> .	
15. Remarks (Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions). STINGER/STINGER-POST Guided Missile System Security Classification Guide dated November 1979 Note: In addition to available guides, instructions may be included on specific requirements required of the contractor such as: "Classified computer usage will be on the user agency's computer located at _____." Whenever possible, contractors should be encouraged to provide input to the preparation of the DD 254.	
Reference item 11n (Classified ADP Processing): When the item is marked yes, include in this remarks section a statement indicating that TEMPEST requirements have been considered and whether they do or do not apply. Include also the identity/title of the individual making that determination, summary of rationale, and location/type of equipment to be used. Submit a copy of the completed DD Form to Cdr, USAINSCOM, ATTN: IAOPS-OP-P, Arlington Hall Sta, Arlington, VA 22212.	
16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below.	
REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> Prime Contractor (Item 7a) <input checked="" type="checkbox"/> Cognizant Security Office (Item 7c) <input checked="" type="checkbox"/> Administrative Contracting Office (Item 16e) <input type="checkbox"/> Quality Assurance Representative <input type="checkbox"/> Subcontractor (Item 8a) <input type="checkbox"/> Cognizant Security Office (Item 8c) <input checked="" type="checkbox"/> Program/Project Manager (Item 12b) <input type="checkbox"/> U. S. Activity Responsible for Overseas Security Administration	b. Typed name and title of approving official JANE S. SMITH Contracting Officer c. Signature  d. Approving official's activity address and Zip Code US Army Missile Command Redstone Arsenal, AL 35809 e. Name, address and Zip Code of Administrative Contracting Office DCASR Plant Representative, XYZ Production Corp 10 Main Street, Los Angeles, CA 90015
ADDITIONAL DISTRIBUTION: <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Figure 1. Example of a completed DA Form 254—Continued

Appendix A References

Section I Required Publications

DOD 5200.1-I

(DOD Index of Security Classification Guides). Cited in paragraph 9.

DOD 5220.22-H

(Handbook for Writing Security Classification Guidance). Cited in paragraph 9.

DOD 5220.22-M

(Industrial Security Manual for Safeguarding Classified Information) (ISM). Cited in paragraphs 6b, 7, B-3a(2)(e) and (i), B-7b(4), and glossary under "closed area", "contracting officer", "restricted area", and "unauthorized person".

DOD 5220.22-R

(Industrial Security Regulation) (ISR)). Cited in paragraphs 5a, 5b(1) and (2), 6a, 6b(1), 7, 7a(1), 7b, 9, and 10a(2), and throughout appendix B.

AR 50-5

Nuclear Surety. Cited in paragraph B-19.

AR 380-5

(DA Information Security Program). Cited in paragraphs 9, B-11, B-12.

AR 380-10

(DA Policy for Disclosure of Military Information to Foreign Governments). Cited in paragraphs B-20, B-23c(1), and B-29a.

AR 380-150

(Access to and Dissemination of Restricted Data). Cited in paragraph B-22.

AR 381-1

(Control of Dissemination of Foreign Intelligence). Cited in paragraphs 8, B-17, and B-21.

Section II Related Publications

This section contains no entries.

Section III Prescribed Forms

This section contains no entries.

Section IV Referenced Forms

This section contains no entries.

Appendix B Supplemental Instruction for the Use of DOD 5220.22-R, Industrial Security Regulation (ISR)

B-1. General.

This appendix contains instructions for using DOD 5220.22-R, Industrial Security Regulation (ISR). The numbers in parentheses identify specific paragraphs in the ISR.

B-2. Authority (1-101).

Recommendation by DA activities for clarification, modification,

additions, deletions, or other changes to the ISR will be forwarded through channels to HQDA (DAMI-CIS).

B-3. Contractor activities on a user-agency installation (1-108a).

DA installation and activity commanders will provide security supervision of contractors and their employees as shown below.

a. For Army installations outside continental United States (OCONUS), Puerto Rico, or US possessions or trust Territories—

(1) The contractor and his employees will be considered as visitors. Procedures developed by installation commanders will vary according to the size and nature of contractor activities. Procedures applying to all aspects of industrial security need not be developed for small integrated contractor activities and those limited contractor operations performed on an installation intermittently or for very short periods of time.

(2) Contractor activity that is extensive in nature and independent in its operation should be given security supervision comparable to that of a cleared contractor facility. In this case, the installation commander will—

(a) Provide written instructions specifying security actions that will be performed for the contractor (for example, providing storage facilities, guard service, mail and freight services, and visit control); and security actions for which joint participation may be required (for example, packaging and addressing of classified transmittals, and visitor control).

(b) Assure that the contractor prepares a standard practice procedure covering contractor activities on the installation, if appropriate.

(c) Assure that the contractor observes required security controls through periodic inspection in accordance with the inspection schedule contained in paragraph 4-103, ISR. Render to contractors requirements resulting from the inspections, if appropriate.

(d) Assure prompt action is taken to correct deficient security conditions noted in the contractor's operation.

(e) Ensure that contractors have a security education program. Conduct, as required, defensive security briefings required by paragraph 5u, ISM.

(f) Investigate contractor security violations, including loss, compromise, or suspected compromise of classified information.

(g) Brief or debrief contractors requiring CRYPTOGRAPHIC access authorizations, where appropriate.

(h) Furnish contractor guidance on the application of security requirements to contractor operations.

(i) Forward requests from contractors for interpretations of the ISM to the cognizant security office, where appropriate.

(j) Request from DISCO interim personnel security clearances for contractor personnel, when required, to prevent crucial delay in performance of the contract.

(k) Assure that the contractor reports promptly any incidents involving espionage, sabotage, subversion, or the loss, compromise, or suspected compromise of classified information.

b. For Army installations located within CONUS, Puerto Rico, or US possessions or trust territories, the contractor and his employees will be considered as visitors. The installation commander also may elect to declare the contractor activity a facility under the criteria of paragraph 1-108a(2)(a) through (d), ISR.

c. (1-108b.) Normally, an installation commander will elect to perform the security actions prescribed by this paragraph only when the contractor's activities are so much a part of the installation's mission and daily operation that it would be impractical to have a DIS Regional Director of Industrial Security perform them.

B-4. Expenditure of funds for security (1-109).

When performing the functions listed in paragraphs 1-108b and 1-108e, ISR, an installation commander will not commit the Government to reimburse a contractor for funds expended in connection with its security program, unless the commander also is responsible for contract performance.

B-5. Disclosure of classified information to a contractor by user agency contracting activities (1-110).

a. Classified information essential to the performance of Army contracts may be released to a contractor facility providing a determination is made that the contractor concerned has—

- (1) A valid security clearance at the appropriate level.
- (2) The need-to-know.
- (3) The capability for proper safeguarding of the information to be released.

b. A contractor's need-to-know for classified information will be certified by the contracting officer, or representative, when appropriate. Potential contractors are considered to have a need-to-know upon submission of evidence and intent to expand to be able to carry out a contract.

c. Classified information intended for release to a contractor will be addressed to the security office of the facility or as specified by the contracting officer.

B-6. Changed security requirements (1-114).

a. Sensitive projects will be supervised as shown below.

(1) Although all Army classified contracts are performed under the security requirements of the DOD Industrial Security Program, a highly sensitive project occasionally may require additional safeguards to ensure the required degree of security. When such a project results in the award of an Army classified contract, that contract may be excluded from the security supervision and inspection of the cognizant security officer. This procedure, known as a "carve-out," is authorized under the following conditions:

(a) The exclusion must be approved in writing by the Army Staff Activity having primary interest in the project or contract.

(b) A specific DA activity must be charged with the responsibility for providing security supervision and inspection over the contractor's performance in the contract. Notification of the establishment of a carve-out will be furnished HQDA (DAMI-CIS).

(2) Before a carve-out procedure is established, every attempt will be made to develop security cognizant functions mutually acceptable to the DA activity and DIS Regional Cognizant Security Office concerned.

(3) Procedures in (2) above will not be interpreted as authority for any DA activity to award a classified contract to any contractor not appropriately cleared under the program.

b. Requests by DA activities for waivers or deviations from ISR or ISM provisions will be submitted to HQDA(DAMI-CIS).

B-7. Security administration of US classified contracts awarded to US contractors for performance abroad (1-115).

a. Army classified contracts awarded for performance outside the United States, its possessions, trust territories, Panama Canal Zone, or Puerto Rico will include appropriate security provisions needed to ensure the proper protection of classified information at the overseas location. Contracting commands will develop (in conjunction with HQDA(DAMI-CIS), the major Army overseas command, and any other command concerned) instructions and guidance pertinent to the performance of the contract overseas. For this purpose, coordination will be effected with the following appropriate office before award of contract:

- (1) CINCUSAREUR
US Army Europe and Seventh Army
ATTN: AEAGB-CI-S
APO NY 09403
- (2) Commanding General
Eighth US Army
ATTN: BJ-IS-S
APO SF 96301
- (3) Commanding General
US Army Japan
ATTN: AJGB-S
APO CA 96343

b. This information will include—

(1) Notification of the Commander of the major overseas command and the Commander of the installation where the contract will be performed when it is let. (See a above for notification address.) This best can be accomplished by including these commands on distribution for the DD Form 254 prepared for such contracts (fig. 1). A copy of any portion of the contract document that prescribes security requirements also will be provided these commands.

(2) Identification of the DA activity that will be responsible for the security supervision and inspection of the contractor's overseas operations.

(3) A requirement to comply with the instructions of the commander of the installation or activity where the contract will be performed.

(4) The transmission channels to be used by the contractor for the shipment of classified material between the United States and the overseas location. (Para 17 of the ISM and para 1-601 of the ISR provide guidance for the transmission of classified information to or from a contractor or contractor employees outside the United States.)

(5) The identity of the US military or the US Government installation where classified information will be stored. Storage of US classified information in a foreign country at a location other than a US military or other US Government-controlled activity is prohibited.

(6) Any other special security instructions pertinent to the security protection of classified information involved in the contract or as required by the major overseas commander.

c. The security supervision of Army classified contracts performed on US military installations overseas is the responsibility of the installation commander.

d. For classified contracts performed at other than US military installations, responsibility for security supervision and inspection of the contractor's operations rests with the appropriate overseas commander having jurisdiction over the area in which the contract is performed. This is true unless arrangements have been made with some other command or agency to fulfill such responsibility.

B-8. Security cognizance—policy (1-300c).

When representatives of Army contracting activities visit a contractor facility to review contract performance, they should inquire into the security aspects of the contract. These visits should be coordinated in advance with the appropriate DIS Regional Cognizant Security Office commander exercising security supervision (under the provisions of para 1-108b).

B-9. Defensive security briefing (1-304).

Army commanders who have elected to perform the functions outlined in paragraph 1-108b, ISR, will arrange to have the contractor submit the reports required by paragraph 5u, ISM, through them to the appropriate cognizant security office. This also applies to Army Commanders who are performing the functions outlined in paragraph 108e, ISR, at an installation outside the United States, its possessions, trust territories, the Panama Canal Zone, and Puerto Rico.

B-10. Responsibility for security of SENSITIVE COMPARTMENTED INFORMATION contracts (1-305c).

When a contract is awarded by and for a DA activity, access to sensitive compartmented information needed by contractor personnel for performance on that contract will be granted by the DA activity designated to exercise security supervision over the contract (for example, US Army Special Security Group, US Army Intelligence and Security Command). (See para 2-315f, ISR).

B-11. Location of meetings (1-404).

DA policy governing the sponsoring, locations and security measures of meetings involving the disclosure of classified information is established in paragraph 5-205, AR 380-5.

B-12. Attendance by foreign nations and representatives of foreign interests.

Requests for attendance at meetings covered in paragraph B-11 by foreign nations and representatives of foreign interests will be forwarded to HQDA(DAMI-CIS), in accordance with paragraph 5-205, AR 380-5.

B-13. Facility security clearances (2-102).

a. Facility clearances may be requested from the appropriate DIS Regional Cognizant Security Office. This may be done when there is a need to enter into precontract negotiations requiring the disclosure of classified information, or to award a classified contract or subcontract. Additionally, clearance may be requested of any facility that is otherwise qualified to be added to the bidder's list, when—

- (1) Future classified procurement is needed.
- (2) The procuring contracting officer determines that costly delays will be caused by waiting for precontract negotiations to begin before initiating facility clearance action.

b. In emergency situations (and to avoid crucial delays in the negotiations, award, or performance of a classified contract), an interim facility clearance may be requested.

(1) DA activities will submit requests for interim CONFIDENTIAL or interim SECRET facility clearances directly to the appropriate DIS Regional Cognizant Security Office.

(2) DA activities will submit requests for interim TOP SECRET facility clearances to the intermediate approving authorities listed below. They are authorized to represent the Secretary of the Army to approve applications to DIS Regional Cognizant Security Offices for interim TOP SECRET facility clearances. This authority may not be further delegated. (See app C for addresses of cognizant security offices.)

Commander in Chief, US Army Europe and Seventh Army.

Commanding General, Eighth US Army.

Commanding General, US Army Materiel Development and Readiness Command (CG, DARCOM).

Commanding General, US Army Training and Doctrine Command (CG, TRADOC).

Commanding General, US Army Communications Command (CG, USACC).

Commanding Generals, CONUS Armies.

Commanding General, US Army Military District, Washington DC (CG, MDW).

Commanding General, US Army Intelligence and Security Command (CG, INSCOM).

Commanding General, US Army Computer Systems Command.

Commanding General, US Army Forces Command (CG, FORSCOM).

Commanding General, US Army Ballistic Missile Defense Systems Command (CG, BMDSCOM).

Commanding General, US Army Western Command (CG, WESTCOM).

Assistant Chief of Staff for Intelligence (ASCI).

(3) The request will include the identity of the DIS Regional Office having security cognizance over the facility; names and positions of company officials requiring interim TOP SECRET clearance in conjunction with interim facility clearance; and a statement justifying the need for the interim clearance.

(4) The approving authority will send the request for interim TOP SECRET facility security clearance to the appropriate DIS Regional Cognizant Security Office as quickly as possible. This transmittal correspondence will state that on the authority delegated by the Secretary of the Army (under para 2-102b, ISR) the DIS Regional Office is authorized to issue the required interim TOP SECRET facility security clearance and related interim TOP SECRET personnel clearances for affected company officials.

B-14. Requirements for security clearances for contractor personnel.

In emergency situations (and in order to avoid crucial delays in the

negotiations, award, or performance of a classified contract), an interim personnel security clearance may be requested.

a. DA activities will submit requests for interim CONFIDENTIAL or interim SECRET personnel security clearance directly to DISCO.

b. The DA activity determining that an interim TOP SECRET clearance is critically needed will submit a request for authorization for such clearance to the appropriate intermediate approving authority designated in paragraph B-13b(2). The request will include name of the individual; level of current security clearance of the individual's contractor facility; and a statement justifying the request.

c. The approving authority will send the request to DISCO as quickly as possible. The transmittal correspondence will state that on the authority delegated by the Secretary of the Army (under para 2-308c(1), ISR), DISCO is authorized to issue the required interim TOP SECRET personnel security clearance.

B-15. Denial of admittance to user agency installations. (2-316).

a. The authority of a commander to control and deny entry to all or part of the installation is absolute. The individual concerned has no right of appeal.

b. When an employee of a cleared DOD contractor has been denied entry or has been removed from an Army-controlled installation for security reasons, this fact will be promptly reported to the Chief, DISCO. An information copy of this report will be forwarded to HQDA (DAMI-CIS).

B-16. Intelligence briefing and debriefing requirements(2-317).

Procedures to be followed by DA activities in the release of intelligence to contractors are in AR 381-1.

B-17. Denial, suspension, or revocation of personnel security clearances (2-320).

Adverse information indicating that the granting or continuance of a contractor employee's security clearance is not clearly consistent with the national interest will be promptly reported to DISCO for appropriate action.

a. Any DA employee who becomes aware of any adverse or derogatory information concerning any contractor employee who has access to classified information will immediately report that information to the local security manager. The security manager will ensure that the information is provided to the commander or head of the user agency responsible for the classified information held by that contractor.

b. When, in the judgment of the responsible Army commander, there is sufficient credible adverse or derogatory information to indicate that continued access to classified information by the contractor employee is not in the best interest of the security of the Army, the commander will—

(1) Take action to recommend an emergency suspension of the contractor employee's security clearance (as prescribed in para 2-320c, ISR).

(2) Take action through the contractor's security officer to immediately deny the employee access to classified information pending resolution of the adverse or derogatory information.

c. Any conflict between DIS and the responsible Army commander concerning access to classified information by any contractor employee will be reported to HQDA(DAMI-CIS) for resolution or suspension of security clearance by the Secretary of the Army.

B-18. Requirements of the Nuclear Weapon Personnel Reliability Program (PRP) (2-324).

See AR 50-5 for DA implementation of the Nuclear Weapon Personnel Reliability Program.

B-19. Visitor categories and procedures (3-103d).

The release of classified information to foreign nationals is governed by AR 380-10.

B-20. Visits to user agency activities in the United States (3-202e).

The release of classified intelligence material to contractors is governed by AR 381-1.

B-21. Visits to DOE installations or DOE contractors (3-301).

Visits by DA personnel to DOE activities are governed by AR 380-150.

B-22. Visits to foreign governments and activities (3-400).

DA activities receiving requests form DISCO for visits by US contractor personnel in the marketing or sales capacity (or in conjunction with a proposal to foreign governments, firms, or foreign nationals involving the release of US classified information) must review each request to determine—

a. If a State Department export license has been issued under the International Traffic in Arms Regulation.

b. Any limitations or restrictions placed on the disclosure of classified information, if appropriate.

c. If the contracting officer and contract are indicated; or, if no contract is involved, the military activity having primary interest in the information concerned. If an export license has been granted (with or without disclosure restriction), no further action by DA is required on the request. This procedure applies to cases involving either classified or unclassified information.

(1) If a State Department export license has been issued, the authority and instruction for the disclosure of classified information will have been granted under AR 380-10. The DA position on the proposed export will have been presented to the Office of Munitions Control, Department of State.

(2) If an export license has not been obtained prior to the submission of the visit request, the visit request will be returned to the contractor with instructions to obtain the required export license in accordance with the International Traffic in Arms Regulation.

(3) When an export license has not been obtained but has been applied for concurrently with the visit request, the visit request will be processed and returned to the contractor with instructions to refrain from initiating or performing any travel on the approved visit request until after the export license has been obtained.

(4) If an export license is not required, the visit may be approved at the discretion of the activity to be visited.

B-23. Use of the DD Form 696 (4-105).

In cases when an installation commander has been elected to perform the security functions listed in paragraph 1-108b, ISR, the DD Form 696 will be used for inspections conducted under the provisions of the ISR. Copies of this form may be obtained from the DIS Regional Office exercising security cognizance over the contractor facility. The use of DD Form 696 on inspections conducted under the provisions of paragraph 1-108e, ISR, is not required.

B-24. Unsatisfactory inspection (4-201a).

a. When an installation commander is performing the security functions listed in paragraph 1-108b, ISR, and determines that there is an immediate danger of compromise of classified information in possession of the contractor, the commander will communicate all the pertinent facts to the following: the DIS Regional Office exercising cognizance over the facility; to HQDA(DAMI-CIS); and to the major contracting command concerned. This also will apply if a facility security inspection conducted under the provisions of section IV, part I, ISR, results in an overall security evaluation of "unsatisfactory." These organizations also will be kept informed of all significant developments.

b. When an installation commander is performing the security functions listed in paragraph 1-108c, ISR, and determines that the

above conditions exist, the commander will take appropriate action to protect the classified information. The commander will report all pertinent facts to the DIS Regional Office which exercises security cognizance over the facility.

c. (4-201b). When a DA contracting officer receives a notification under the provisions of this paragraph, the contracting commander will render all possible assistance to the DIS Regional Cognizant Security Office concerned to enforce the security obligation of the contract.

(1) The contracting officer will not release any additional classified information to the facility until the deficient condition has been corrected. Continued release may be authorized by the Secretary of the Army, based on a determination that continuation of the contract is so essential that national interest must prevail over security considerations.

(2) In cases of continuing failure to maintain required standards, or upon request of the DIS Regional Cognizant Security Office, the contracting officer will withdraw the classified information already in the custody of the facility.

(3) If warranted, the contracting command, (in coordination with the DIS Regional Cognizant Security Office having jurisdiction over the facility) will initiate action to terminate the classified contract by default. Consideration also will be given to initiating action to debar or suspend the contractor.

B-25. Investigative support (5-103).

Investigative support (5-103). The CG, INSCOM will provide investigative support when requested by the DIS Regional Cognizant Security Office in accordance with paragraph 5-103b, ISR. Requests for such support will be limited to cases involving RESTRICTED DATA or FORMERLY RESTRICTED DATA in which the DIS Cognizant Security Office suspects that a criminal violation of the Atomic Energy Act of 1954 has occurred; or a need for special investigative technique exists. In those instances the case file with related reports will be submitted to CG, INSCOM (ATTN: IASO), Fort Meade, MD 20755. Copies of such referrals will be sent to the contracting officer; the DIS Regional Director; Director, DIS (ATTN: Director Industrial Security); and HQDA(DAMI-CIS).

B-26. Training schools (6-106).

The Director for Industrial Security, DIS will budget and fund for industrial security training courses conducted by the Defense Industrial Security Institute (DISI).

B-27. Review of classification and need-to-know (7-104).

Contracting commands will ensure that security classification guidance furnished to contractors is reviewed as required by this paragraph. When procurement responsibility passes from one command to another, the receiving command will assume this responsibility.

B-28. Procedure for the security of US classified contracts or subcontracts awarded to a foreign contractor (8-104a).

a. Agreements referred to in this paragraph signify that the foreign government concerned places the responsibility on its contractors to properly safeguard US classified information, for clearing the contractor and the contractor's employees, and other security measures rests with the foreign government or agency as authorized under this paragraph. The contracting commander will assure that any classified information involved in the contract has been approved for release in accordance with AR 380-10.

b. (8-104b). Although the foreign government concerned is responsible for security inspections of the contractor's operations, if the contract is performed on an installation under US control, these inspections will be conducted by the appropriate US military authority. Arrangements will be made to provide for this inspection procedure and to guarantee the US military commander continuing security of the installation.

B-29. Industrial security forms (9-100).

Industrial security forms (9-100). Industrial security forms needed

by installation commanders to accomplish cognizant security functions will be obtained from the appropriate DIS Regional Cognizant Security Office.

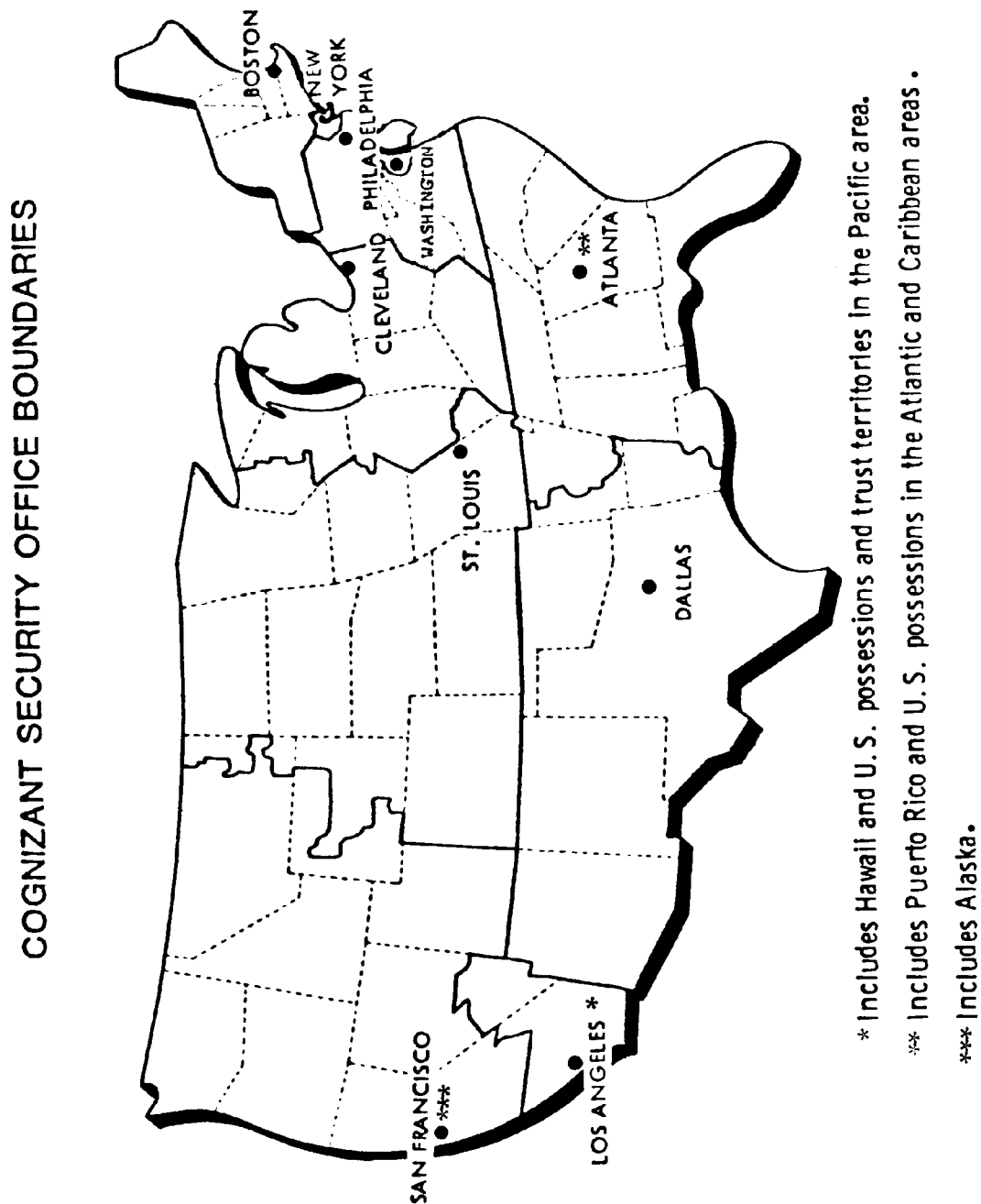


Figure C. Cognizant Security Office Boundaries

Operational Areas of DIS Cognizant Security Offices

ATLANTA

States of: North Carolina, South Carolina, Georgia, Tennessee, Mississippi, Alabama, Florida, Kunkin and Pemiseot counties in Missouri, also includes Puerto Rico and U.S. possessions in the Atlantic and Caribbean areas, and the following counties in Arkansas:

Arkansas	Jackson
Baxter	Jefferson
Boone	Lawrence
Bradley	Lee
Calhoun	Lincoln
Clay	Lonoke
Cleburne	Marion
Cleveland	Mississippi
Conway	Monroe
Craighead	Newton
Crittenden	Perry
Cross	Phillips
Dallas	Poinsett
Deska	Prairie
Drew	Pulaski
Faulkner	Randolf
Fulton	Saint Francis
Garland	Saline
Grant	Searcy
Greene	Sharp
Hot Springs	Stone
Independence	Van Buren
Izard	White
	Woodruff

The following counties in Louisiana:

Ascension	Saint Charles
Assumption	Saint Helena
East Baton Rouge	Saint James
East Feliciana	Saint John the Baptist
Iberia	Saint Martin
Iberville	Saint Mary (and part of Saint Martin)
Jefferson	Saint Tammany
Lafayette	Tangipahoa
LaFourche	Terrebonne
Livingston	Vermilion
Orleans	Washington
Plaquemines	Wesr Baton Rouge
Pointe Coupee	West Feliciana
Saint Bernard	

BOSTON

States of Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut, and the following counties in New York:

Albany	Columbia
Allegany	Cortland
Broome	Delaware
Cattaraugus	Dutchess
Cayuga	Erie
*Chautaugua	Essex
Chemung	Franklin
Chenango	Fulton
Clinton	Genesee
Greene	Saratoga
Hamilton	Schenectady
Herkimer	Schoharie
Jefferson	Schuyler
Lewis	Seneca
Livingston	Steuben
Madison	Sullivan
Monroe	Tioga
Montgomery	Tompkins

The following counties in New York:—Continued

Niagara	Ulster
Oneida	Warren
Onondaga	Washington
Ontario	Wayne
Orleans	Wyoming
Oswego	Yates
Otsego	
Rensselaer	
Saint Lawrence	

WASHINGTON

The counties of Hartford, Baltimore, Howard, Anne Arundel, Montgomery, Prince George's, Calvert, Saint Mary's and Charles in Maryland, and the counties of Loudoun, Fairfax, Prince William, Arlington, in Virginia, and Washington, D.C., and the city of Alexandria, Va.

CLEVELAND

States of Ohio, Kentucky, Indiana, Michigan, and the counties of Marshall, Ohio, Brooke and Hancock in West Virginia, and the counties of Jackson, Clinton, Scott, and Muscatine in Iowa, and the following counties in Wisconsin:

Adams	Marathon
Ashland	Marinette
Brown	Marquette
Calumet	Menominee
Clark	Monroe
Columbia	Oconto
Crawford	Oneida
Dane	Outgamie
Dodge	Ozaukee
Door	Portage
Florence	Price
Forest	Racine
FondduLac	Richland
Grant	Rock
Green	Sauk
Green Lake	Shawano
Iron	Sheboygan
Iowa	Taylor
Juneau	Vernon
Kewaunee	Vilas
Kenosha	Walworth
LaCrosse	Washington
Lafayette	Waukesha
Langlade	Waupaea
Lincoln	Waushara
Manitowoc	Winnebago
Milwaukee	Wood

The following counties in Illinois:

Adams	Effingham
Boone	Ford
Brown	Fulton
Bureau	Grundy
Carroll	Hancock
Cass	Henderson
Champaign	Henry
Christian	Iroquois
Clark	Jasper
Coles	Jo Daviess
Cook	Kane
Crawford	Kankakee
Cumberland	Kendall
DeKalb	Knox
DeWitt	Lake

The following counties in Illinois:—Continued

Douglas	La Salle
DuPage	Lee
Edgar	Livingston
Logan	Putnam
Macon	Rock Island
Marshall	Sangamon
Mason	Schuyler
McDonough	Scott
McHenry	Shelby
McLean	Stark
Menard	Stephenson
Mercer	Tazewell
Morgan	Vermillion
Moultrie	Warren
Ogle	Whiteside
Peoria	Will
Piatt	Winnebago
Pike	Woodford

DALLAS

States of: New Mexico, Texas, Oklahoma, Arizona, and the following counties in Arkansas:

Benton	Miller
Carroll	Montgomery
Clark	Nevada
Columbia	Ouachita
Crawford	Pike
Franklin	Polk
Hempstead	Pope
Howard	Scott
Johnson	Sebastian
Lafayette	Sevier
Little River	Union
Logan	Washington
Madison	Yell

The following counties in Louisiana:

Acadia	De Soto
Allen	East Carroll
Avoyelles	Evangeline
Beauregard	Franklin
Bienville	Grant
Bossier	Jackson
Caddo	Jefferson Davis
Calcasieu	La Salle
Caldwell	Lincoln
Cameron	Madison
Catahoula	Morehouse
Claiborne	Natchitoches
Concordia	Ouachita
Rapides	Union
Red River	Vernon
Richland	Webster
Sabine	West Carroll
Saint Landry	Winn
Tensas	

LOS ANGELES

Includes state of Hawaii & U.S. possessions & trust territories in the Pacific area, and the following counties in California:

Imperial	San Bernadino
Inyo	San Diego
Kern	San Luis Obispo
Los Angeles	Santa Barbara

The following counties in California:—Continued

Orange	Ventura
Riverside	

The following counties in Nevada:

Clark	Lincoln
Esmeralda	Nye

NEW YORK

The following counties in New York:

Bronx	Putnam
Kings	Queens
(Brooklyn)	Richmond
Nassau	Rockland
New York	Suffolk
(Manhattan)	Westchester
Orange	

The following counties in New Jersey:

Bergen	Morris
Essex	Passaic
Hudson	Somerset
Hunterdon	Sussex
Middlesex	Union
Monmouth	Warren

PHILADELPHIA

States of: Pennsylvania, Delaware, West Virginia (less the counties of Marshall, Hancock, Brooks and Ohio), Virginia (less the counties of Loudoun, Fairfax, Prince William and Arlington), Maryland (less the counties of Hartford, Baltimore, Howard, Anne Arundel, Montgomery, Prince George's, Calvert, Saint Mary's and Charles), Chautauqua county in New York, and the following counties in New Jersey:

Atlantic	Camden
Burlington	Cape May
Cumberland	Ocean
Gloucester	Salem
Mercer	

SAINT LOUIS

States of: N. Dakota, S. Dakota, Minnesota, Nebraska, Colorado, Kansas, Missouri (less Dunkin and Pemiscot counties), Iowa (less Jackson, Clinton, Scott and Muscatine counties), and the following counties in Wisconsin:

Barron	Burnett
Bayfield	Chippewa
Buffalo	Douglas
Dunn	Polk
Eau Claire	Rush
Jackson	Saint Croix
Pepin	Sawyer
Pierce	Trempealeau
	Washburn

The following counties in Montana:

Carter	Prairie
Daniels	Roosevelt
Dawson	Richland
McCone	Sheridan
Powder River	Wibaux

The following counties in Wyoming:

Albany	Fremont
Cambell	Goshen
Carbon	Laramie
Converse	Natrona
Crook	Niobrara
Platte	Weston

The following counties in Illinois:

Alexander	Jacks
Bond	Jefferson
Calhoun	Jersey
Clay	Johnson
Clinton	Lawrence
Edwards	Macoupin
Fayette	Madison
Franklin	Marlon
Gallatin	Massac
Green	Monroe
Hamilton	Montgomery
Hardin	Perry
Pope	Union
Pulaski	Wabash
Randolph	Washington
Richland	Wayne
St. Clair	White
Saline	Williamson

SAN FRANCISCO

States of: Washington, Oregon, Idaho, Utah, Alaska, and the following counties in Wyoming:

Big Horn	Sublette
Hot Springs	Sweetwater
Johnson	Teton
Lincoln	Uinta
Park	Washakie
Sheridan	

The following counties in Montana:

Beaverhead	Broadwater
Big Horn	Carbon
Blaine	Cascade
Chauteau	Mineral
Custer	Missoula
Deer Lodge	Musselshell
Fallon	Park
Fergus	Petroleum
Flathead	Phillips
Gallatin	Pondera
Garfield	Powell
Glacier	Ravalli
Golden Valley	Rosebud
Granite	Sanders
Hill	Silver Bow
Jefferson	Stillwater
Judith Basin	Sweet Grass
Lake	Teton
Lewis and Clark	Toole
Liberty	Treasure
Lincoln	Valley
Madison	Wheatland
Meagher	Yellowstone

The following counties in Nevada:

Churchill	Lyon
Douglas	Mineral
Elko	Pershing
Eureka	Storey
Humboldt	Washoe

The following counties in Nevada:—Continued

Lander	White Pine
--------	------------

The following counties in California:

Alameda	Nevada
Alpine	Placer
Amador	Plumas
Butte	Sacramento
Calaveras	San Benito
Colusa	San Francisco
Contra Costa	San Joaquin
Del Norte	San Mateo
El Dorado	Santa Clara
Fresno	Santa Cruz
Glenn	Shasta
Humboldt	Sierra
Kings	Siskiyou
Lake	Solano
Lassen	Sonoma
Madera	Stanislaus
Marin	Sutter
Mariposa	Tehama
Mendocino	Trinity
Merced	Tulare
Modoc	Tuolumne
Mono	Yolo
Monterey	Yuba
Napa	

TELEPHONE NUMBERS AND ADDRESSES

The following listing contains the addresses and telephone numbers of all Cognizant Security Offices. (The following indicated telephone numbers and addresses shall be used to obtain the required verification of facility clearance and safeguarding capability of prospective contractors and subcontractors.)

City & State	Address	Area Code	Telephone Number
Atlanta, GA	805 Walker St. Marietta, GA 30060	404	429-6340
Boston, MA 02210	666 Summer Street	617	542-6000, ext 838
Cleveland, OH 44199	Federal Office Bldg. 1240 East 9th Street	216	522-5338/9
Dallas, TX 75201	Merchandise Mart Bldg. 500 South Ervay Street	214	670-9276
Los Angeles, CA 90045	11099 S. LaCienega Blvd.	213	643-0203
New York, NY 10013	60 Hudson Street	212	374-9040
Philadelphia, PA 19101	P.O. Box 7478 2800 South 20th Street	215	952-4030
San Francisco, CA 94129	Presidio of San Francisco	415	561-6235
St. Louis, MO 63101	1136 Washington Street	314	263-6581
Washington, D.C. (Capital Region)	2461 Eisenhower Ave. Alexandria, VA 22331	202	325-9616

Cognizant Security Office	Area Code	Telephone Number	AUTOVON NO. (For Govt. Agencies Use)
Atlanta	404	429-6340	697-6340
Boston	617	542-6000, ext. 805	955-8805
Cleveland	216	522-5334	580-5334
Dallas	214	670-9270	940-1270
Los Angeles	213	643-1082	833-1082
New York	212	374-9040	994-9046
Philadelphia	215	952-4030	444-4030
San Francisco	415	561-3572	586-6235
St. Louis	314	263-6580	693-6580
Washington (Capital Region)	202	325-9161	221-9616

The following listing contains the addresses and telephone numbers of DISCO, DISI and OISI.

City & State	Address	Area Code	Telephone Number
DISCO, Columbus, OH 43216	P.O. Box 2499	614	236-2133 (Duty Hrs)
		614	236-2058 (After Hrs)
	AUTOVON NUMBER (For Govt. Agencies Use)		850-2133 (Duty Hrs)
DISI, Richmond, VA 23297	c/o Defense General Supply Center	804	275-4891
	AUTOVON NUMBER (For Govt. Agencies Use)		695-4891
OISI, Brussels, Belgium	Physical Address: Office of Industrial		Brussels, Belgium 720-8259
	Security, International		
	Chaussee de Louvain, 13		
	1940 St. Stevens, Woluwe, Belgium		
	Mailing Address: Office of Industrial		
	Security, International		
	APO New York 09667		

Glossary

Section I Abbreviations

This section contains no entries.

Section II Terms

Access, accessibility.

The ability and opportunity to obtain knowledge of classified information. Access to classified information may be gained by being in a place where such information is kept, if the security measures in force do not prevent unauthorized disclosure.

Alien.

Any person not a citizen or national of the United States.

Authorized persons.

Those persons who have need-to-know for the classified information involved and have been cleared for the receipt of such information. A person's duties may require that he possess, or have access to, classified information; whether this person is authorized to receive it rests upon the individual who has possession, knowledge, or control of the information involved and not upon the prospective recipient.

Candidate Material.

That material which is referred to collectively as special nuclear material and nuclear weapons.

Central office of record.

The DOD or user agency activity to which an accounting and reports for accountable COMSEC material are required for a particular contract.

Classified contract.

Any contract that requires (or will require) access to classified information by the contractor or his employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.)

Classification guides.

Guidance issued or approved by an original TOP SECRET classification authority that identifies information or material to be protected from unauthorized disclosure; it also specifies the level and duration of classification assigned or assignable to such information or material under authority of Executive Order 12065. Classification guides are provided to contractors by DD Form 254. (See fig. 1.)

Classified information.

Information or material that is owned by, and produced by, for, or under the control of the US Government (pursuant to E.O. 12065) or

prior orders to require protection against unauthorized disclosure, and is so designated.

Classifier.

An individual who makes a classification determination and applies a security classification to information or material. A classifier may be a classification authority or may have derivative authority to assign a security classification based on a properly classified source or classification guide. Within this context, contractors may apply security classification markings based on classified source material or a DD Form 254. (See fig. 1.)

Closed area.

A controlled area established to safeguard classified material which, because of its size or nature, cannot be adequately protected by the safeguards prescribed in paragraph 16, ISM, or be stored during non-working hours in accordance with paragraph 14, ISM. (See sec IV, ISM.)

Cognizant security office.

The DIS (Director of Industrial Security) having industrial security jurisdiction over the geographic area in which a facility is located.

College and universities.

All educational institutions which award academic degrees and their related research activities directly associated therewith through organizations or by articles of incorporation.

Communications intelligence.

Technical and intelligence information derived from foreign communications by other than the intended recipients.

Communications security (COMSEC).

The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to communications and from the application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value, that might be derived from possession and study of such communications, or to ensure the authenticity of such communications.

Communications security (COMSEC) information.

All information concerning COMSEC and all material (documents, devices, maintenance manuals, and equipment or apparatus) including Cryptomaterial associated with the security or authenticity of telecommunications.

Compromise.

The disclosure of classified information to persons not authorized access to it.

Compromising emanations.

Unintentional data related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmitted, received, handled, or otherwise

processed by electrically operated information processing equipment's or systems.

CONFIDENTIAL.

The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security.

Continental limits of the United States.

US territory, including adjacent territorial waters within the North American continent between Canada and Mexico.

Contracting officer.

A person who, in accordance with departmental or agency procedures, is currently designated a contracting officer, with the authority to enter into and administer contracts and make determinations and findings with respect to them or any part of such authority. The term also includes the authorized representative of the contracting officer acting within the limits of his authority. For purposes of this regulation and the ISM, the term "contracting officer" refers to the person at the purchasing office identified as the procuring contracting officer (PCO) and the person at a contract administration office identified as the administrative contracting officer (ACO).

Contractor.

An entity (industrial, educational, commercial, or other) that has executed a contract with a user agency or a DD Form 441 with a DOD agency or activity.

Critical Nuclear Weapon Design Information (CNWDI).

That TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable and high-explosive materials by type. Among excluded items are the components which DOD personnel (including contractor personnel) set, maintain, operate or replace.

CRYPTO.

A designation or marking that identifies classified operational keying material, indicating that this material requires special consideration with respect to access, storage, and handling.

CRYPTOGRAPHIC System.

The associated items of cryptomaterial used as a unit, providing a single means of encryption and decryption.

Custodian.

An individual who has possession of (or is otherwise charged with) the responsibility for

safeguarding or accounting for classified information.

Declassification.

The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

Derivative classification.

A determination that information is in substance the same as information that is currently classified and a designation of the level of classification.

Document.

Any recorded information, regardless of its physical form or characteristics (exclusive of machinery, apparatus, equipment, or other items of material). The term "document" includes, but is not limited to written material, whether handwritten, printed, or typed; photographs, negatives, exposed or printed films, and still or motion pictures; data processing cards or tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; reproduction of the foregoing by whatever process reproduced; and sound, voice, or electronic recordings in any form.

Downgrade.

To determine that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

Executive personnel.

Those individuals in managerial positions (other than owners, officers, or directors) who administer the operations of the facility. This term includes general manager, plant manager, plant superintendent, or similar designations and facility security supervisor.

Facility.

A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components which, when related by function and location, forms an operating entity. (A business or educational organization may consist of one or more of these facilities.) For purposes of industrial security, the term "facilities" does not include user agency installations.

Facility security clearance.

An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

Foreign government information.

Information that is:

a. Provided to the United States by a foreign government or international organization of governments in the expectation (express or

implied) that the information is to be kept in confidence.

b. Produced by the United States pursuant to written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement (or both) be kept in confidence. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record.

Foreign interest.

Any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the United States, or its possessions; any form of business enterprise organized or incorporated under the laws of the United States, or a State or other jurisdiction of the United States, but owned or controlled by a foreign government, firm, corporation, or person. The term "foreign interest" also includes any natural person who is not a citizen or national of the United States. (An "immigrant alien" as explained below is excluded from the explanation of a foreign interest.)

Foreign nationals.

All persons not citizens of, nor nationals of, nor immigrant aliens to, the United States.

Graphic arts.

Facilities and individuals engaged in performing consultation, service, or the production of any component or end product that contributes or results in the reproduction of classified information. Regardless of trade names or specialized processes, the term "graphic arts" includes writing, illustrating, advertising services, copy preparation, all methods of printing, finishing services, duplicating, photocopying, and film processing activities.

Handling.

The preparation, processing, transmission, and custody of classified information.

Home office.

The headquarters facility of a multiple facility organization.

Immigrant alien.

Any person lawfully admitted into the United States under an immigration visa for permanent residence.

Industrial security.

That portion of internal security that is concerned with the protection of classified information in US industry.

Information security.

The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure. Protection of this information is authorized by Executive Order or statute.

Intelligence.

The product resulting from collection, evaluation, analysis, integration, and interpretation of available information that concerns one or more aspects of foreign nations or of areas of foreign operations. Intelligence is immediately or potentially significant to military planning and operations.

Interim security clearance.

A clearance based on lesser investigative requirements. It is granted on a temporary basis, pending the completion of the full investigative requirements.

Internal security.

The prevention of action against US resources, industries, and institutions; and the protection of life and property in the event of a domestic emergency by the employment of measures, in peace or war, other than military defense.

Locked entrance.

An entrance to a closed or restricted area that is kept closed and locked at all times; except when temporarily unlocked and opened under supervision for passing material or authorized personnel into or out of the area.

Long title.

The full title or name assigned to a publication, an item or equipment, or device.

Material.

Any product or substance on, or in, which information is embodied.

Multiple facility organization.

A legal entity (single proprietorship, partnership, association, trust, or corporation) composed of two or more facilities.

National of the United States.

a. A citizen of the United States.
b. A person who, although not a citizen of the United States, owes permanent allegiance to the United States.

NATO classified information.

All classified information (military, political, and economic) circulated within and by NATO, whether such information originates in the organization itself or is received from member nations or from other international organizations.

Need-to-know.

A determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to knowledge of (or possession of) the classified information, in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a user agency.

Negotiator.

Any employee, in addition to the owners, officers, directors, and executive personnel (OODEPs), who requires access to classified

information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime or subcontract. The term "negotiator" may include, but is not limited to, accountants, stenographers, clerks, engineers, draftsmen, and production personnel.

Officers (corporation, association, or other types of business or educational institution).

Those persons in positions established as officers in the articles of incorporation or by-laws of the organization.

Official information.

Information that is owned by, produced for or by, or is subject to the control of the US Government.

Parent firm.

A corporation that can control another corporation (subsidiary) by ownership of a majority of its stock. The control may exist by direct stock ownership of an immediate subsidiary or by indirect ownership through one or more intermediate levels of subsidiaries.

Possessions.

Possessions include the Virgin Islands, Guam, American Samoa, and the Guano Islands with Swains Island, Howland Island, Baker Island, Jarvis Island, Midway Islands, Kingman Reef, Johnston Island, Sand Island, Navassa Island, Swan Islands, and Wake Island.

Principal management facility.

A cleared facility of a multiple facility organization that reports directly to the home office. The facility's principal management official also has been delegated the responsibility to administer the contractor's industrial security program, within a defined geographical and functional area.

Reference material.

Documentary material over which the user agency does not have classification jurisdiction at the time such material was originated. Much material made available to the contractors by the Defense Technical Information Center and other secondary distribution agencies is reference material as explained.

Regrade.

To assign a higher or lower security classification to an item of classified material.

Representatives of a foreign interest.

Citizens or nationals of the United States or immigrant aliens who, in their individual capacity, or on behalf of a corporation (whether as a corporate officer or official, or as a corporate employee personally involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, or person. However, a US citizen or national who has been appointed by his/her US employer to be

its representative in the management of a foreign subsidiary (for example, a foreign firm in which the US firm has ownership of at least 51 percent of the voting stock) will not be considered a representative of a foreign interest, solely because of this employment. (Provided the appointing employer is his principal employer and is a firm that possesses or is in process for a facility security clearance.)

Restricted areas.

Controlled areas established to safeguard classified material which, because of its size or nature, cannot be adequately protected during working hours by the safeguards prescribed in paragraph 16, ISM, but which is capable of being stored during non-working hours, in accordance with paragraph 14, ISM. (See sec IV, ISM.)

SECRET.

The designation applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include: disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

Security.

The safeguarding of information classified TOP SECRET, SECRET, or CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.

Security cognizance.

The responsibility for acting for user agencies in the discharge of industrial security responsibilities.

Sensitive compartmented information.

Information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs; their end products for which community systems of compartmentation have been or will be formally established. (The term does not include RESTRICTED DATA as explained in section II, Public Law 585, Atomic Energy Act of 1954, as amended.)

Short title.

An identifying combination of letters and numbers assigned to a publication or equipment for brevity.

Special access program.

Any program imposing need-to-know or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, OR TOP SECRET information. Such a program includes, but is not limited to, special

clearance, adjudication, or investigative requirements, material dissemination restrictions, or special lists or persons determined to have "need-to-know."

Subsidiary.

A corporation that is controlled by another corporation (parent) by reason of the latter corporation's ownership of at least a majority (over 50 percent) of the capital stock. A subsidiary is legal entity and will be processed separately for a facility security clearance.

Telecommunications.

Any transmission, emission, or reception of signs, signals, writings, images, and sound, or intelligence of any nature by wire, radio, visual, or other electromagnetic system.

Time resource sharing.

The concurrent use of an automatic data processing (ADP) system by one or more users. The term includes the functional characteristics of an ADP system that allow simultaneous or apparently simultaneous access to all or part of an ADP system by more than one user; or the acceptance and processing of more than one computer program of instructions. The term encompasses the characteristics of time sharing, multiprocessing, or combinations of those functional capabilities, in any form.

TOP SECRET.

The designation applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include: armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital material defense plans or complex cryptologic and communications defense systems; the revelation of sensitive intelligence operations; and the disclosure of scientific and technological developments vital to national security.

Transmission security.

That component of security that results from all measures designed to protect communication transmission from interception and traffic analysis.

Trust Territory.

The Trust Territory of the Pacific Islands which the United States administers under the terms of a trusteeship agreement concluded between the US Government and the Security Council of the United Nations pursuant to authority granted by Joint Resolution of Congress, July 18, 1947 (61 Stat. 397; 48 U.S.C., Section 1681). According to this agreement, the United States has "full power of administration, legislation, and jurisdiction." Three major archipelagoes make up this Trust Territory: Carolines (including the Palau Islands), Marshalls, and Marianas (excluding Guam).

Unauthorized person.

Any person not authorized to have access to specific classified information in accordance with the provisions of the ISM and this regulation.

Unites States.

The 50 States and the District of Columbia.

Upgrade.

To determine that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher degree.

User agencies.

These agencies are explained below.

a. The Office of the Secretary of Defense (OSD) (including all boards, councils, staffs, and commands).

b. DOD agencies and Departments of the Army, Navy, and the Air Force (including all of their activities).

c. The National Aeronautics and Space Administration (NASA), General Services Administration (GSA), Small Business Administration (SBA), National Science Foundation, Environmental Protection Agency, and Federal Energy Administration.

d. The Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Health and Human Services, Labor, and Justice.

e. U.S. Arms Control and Disarmament Agency and the Federal Emergency Management Agency (FEMA).

Section III**Special Abbreviations and Terms**

There are no special terms.

UNCLASSIFIED

PIN 004089-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.64

PIN: 004089-000
DATE: 03-22-00
TIME: 17:06:53
PAGES SET: 22

DATA FILE: t142.fil
DOCUMENT: AR 380-49
DOC STATUS: REVISION